DETECTION AND MITIGATION OF JAMMING ATTACKS IN MASSIVE MIMO SYSTEMS USING RANDOM MATRIX THEORY

Julia Vinogradova, Emil Björnson and Erik G Larsson

Vinogradova, J., Björnson, E., Larsson, E. G, (2016), DETECTION AND MITIGATION OF JAMMING ATTACKS IN MASSIVE MIMO SYSTEMS USING RANDOM MATRIX THEORY, *2016 IEEE 17TH INTERNATIONAL WORKSHOP ON SIGNAL PROCESSING ADVANCES IN WIRELESS COMMUNICATIONS (SPAWC)*. https://doi.org/10.1109/SPAWC.2016.7536868

Original publication available at:
https://doi.org/10.1109/SPAWC.2016.7536868

DETECTION AND MITIGATION OF JAMMING ATTACKS IN MASSIVE MIMO SYSTEMS USING RANDOM MATRIX THEORY

Julia Vinogradova, Emil Björnson, and Erik G. Larsson

Department of Electrical Engineering (ISY), Linköping University, Sweden

ABSTRACT

Consider the uplink of a single-cell multiuser MIMO system with a very large number of antennas, M, at the base station (BS) and K single-antenna users. A jamming device equipped with K^{J} antennas transmitting signals attempts to degrade the transmission between the users and the BS. In this paper, we propose a detection algorithm of the jamming attack as well as a method for its rejection. The proposed results are based on the application of results from random matrix theory. We assume that K and K^{J} are fixed as M converges to infinity while the coherence interval τ is assumed to be of the same order of magnitude as M.

Index Terms— Massive MIMO, jamming attack, detection, random matrix theory

I. INTRODUCTION

Massive MIMO is an emerging technology allowing to improve the spectral efficiency of wireless communication systems and has been considered as a key candidate for the next generation wireless systems. In addition to an improved spectral and energy efficiency, other advantages of massive MIMO are enhanced reliability and reduced interference [1]. Moreover, due to the large number of degrees of freedom offered in massive MIMO, its robustness to jamming attacks was conjectured in [1]. Indeed, a promising analysis of jamming and eavesdropping attacks was conducted in [2], [3]. It was shown in [3] that the secure degree of freedom achieved in the presence of jamming and eavesdropping attacks is the same as under no attack. Nevertheless, it was pointed out (see, *e.g.*, [2], [3]) that massive MIMO is particularly vulnerable to attacks during the pilot transmission phase making the channel estimation highly degraded. This is referred to as a pilot contamination attack.

In downlink transmission, the effect of pilot contamination attacks was analysed in [3]. It was shown in [3] that a maximum secure degree of freedom is zero when the pilot signals are jammed. In uplink, the impact of smart jamming optimally allocating its power budget to jam the pilot and data transmission was studied in [4] demonstrating a spectacular loss in the sum spectral efficiency when the BS acts as if there is no jamming. One of the most relevant challenges in dealing with jamming attacks is their detection because the jammer can smartly adapt its transmission power in order to avoid to be observed. However, even if its presence is detected, mitigation of the jamming impact is still an open problem in massive MIMO.

In this paper, we propose two algorithms:

1) Jamming detection: a multiple hypothesis testing approach is taken in order to detect the presence of the jamming attack by analyzing the spectrum of the received sample covariance matrix;
2) Jamming mitigation: the eigensubspace corresponding to the K users is identified from the received sample covariance matrix, and the received signal is projected to this subspace to mitigate jamming.

The proposed algorithms are based on the application of some known results from random matrix theory. More specifically, our approach is based on the assumption of a fixed number of users and fixed number of jamming antennas as M converges to infinity.

Notations: The superscript $(\cdot)^{\mathsf{H}}$ is the Hermitian transpose of a matrix. We denote by $\xrightarrow{\text{a.s.}}$ the almost sure (a.s.) convergence. We denote by $\mathcal{CN}(\mathbf{a}, \mathbf{\Sigma})$ the multivariate complex normal distribution with mean $\mathbf{a}$ and covariance matrix $\mathbf{\Sigma}$.

II. TRANSMISSION SCENARIO

Consider a single-cell multiuser MIMO system containing a BS equipped with M antennas and K single-antenna users. This is depicted in Fig. 1 where there are also K^{J} distributed (or co-located) single-antenna jamming devices.

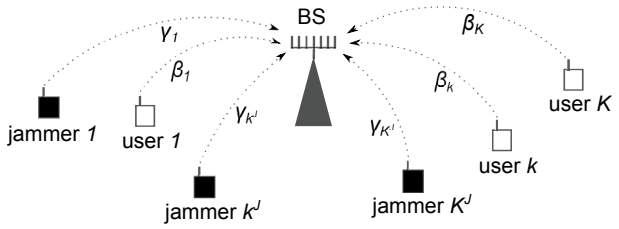

Fig. 1. Distributed jamming of the uplink in a single cell containing K single-antenna users (with pathlosses $\beta_1, \ldots, \beta_K$) and K^{J} single-antenna jamming devices (with pathlosses $\gamma_1, \ldots, \gamma_{K^{\mathsf{J}}}$).

We consider the uplink transmission where the BS receives signals from the K users. The transmitted data vector $\mathbf{x}_t \in \mathbb{C}^{K \times 1}$ at time t is assumed to have independent entries with $\mathbf{x}_t \sim \mathcal{CN}(\mathbf{0}, \mathbf{P})$ where $\mathbf{P} = \text{diag}(P_1, \ldots, P_K)$

978-1-5090-1749-2/16/$31.00

with $P_1 \geq \ldots \geq P_K$ representing the received[1] powers of the transmitted signals; $\mathbf{H} \in \mathbb{C}^{M\times K}$ is the channel matrix between the BS and the K users with independent identically distributed (i.i.d.) entries $\mathbf{H}_{m,k} \sim \mathcal{CN}(0,1)$; $\mathbf{x}_t^{\mathsf{J}} \in \mathbb{C}^{K^{\mathsf{J}}\times 1}$ is the jamming data vector with independent entries with $\mathbf{x}_t^{\mathsf{J}} \sim \mathcal{CN}(\mathbf{0}, \mathbf{P}^{\mathsf{J}})$ where $\mathbf{P}^{\mathsf{J}} = \mathrm{diag}(P_1^{\mathsf{J}}, \ldots, P_{K^{\mathsf{J}}}^{\mathsf{J}})$ with $P_1^{\mathsf{J}} \geq \ldots \geq P_K^{\mathsf{J}}$ representing the jamming received power at each antenna k^{J}; $\mathbf{H}^{\mathsf{J}} \in \mathbb{C}^{M\times K^{\mathsf{J}}}$ is the channel matrix between the BS and the jammer with entries $\mathbf{H}_{m,k^{\mathsf{J}}}^{\mathsf{J}} \sim \mathcal{CN}(0,1)$. Finally, the additive noise is represented by the vector $\mathbf{w}_t \in \mathbb{C}^{M\times 1}$ with $\mathbf{w}_t \sim \mathcal{CN}(\mathbf{0}, \sigma^2\mathbf{I}_M)$. The length of the coherence interval is denoted by τ. We further assume that M and τ are both large converging to infinity such that $M/\tau \to c > 0$ and denote this asymptotic regime by $M \to \infty$. Moreover, K and K^{J} are assumed to be fixed as $M \to \infty$. Before presenting the proposed algorithms for jamming detection and rejection we provide some preliminary results from random matrix theory.

III. PRELIMINARIES

The approach of this paper is based on results on the largest eigenvalues' behavior of large-dimensional random matrices. Let us first consider the matrix $\mathbf{W} \in \mathbb{C}^{M\times\tau}$ with i.i.d. entries such that $\mathbf{W}_{m,t} \sim \mathcal{CN}(0,\sigma^2)$. It is well known (see, *e.g.*, [5]) that as $M \to \infty$, such that $M/\tau \to c > 0$, the spectrum of the sample covariance matrix $\frac{1}{\tau}\mathbf{W}\mathbf{W}^{\mathsf{H}}$ converges to the Marčenko–Pastur (MP) law with the support $[a,b]$ with $a \triangleq \sigma^2(1-\sqrt{c})^2$ and $b \triangleq \sigma^2(1+\sqrt{c})^2$. Moreover, from [6], a.s., no eigenvalue of $\frac{1}{\tau}\mathbf{W}\mathbf{W}^{\mathsf{H}}$ can be found outside the interval $[a,b]$ as M grows large. The following theorem provides the fluctuations of the largest eigenvalue of $\frac{1}{\tau}\mathbf{W}\mathbf{W}^{\mathsf{H}}$.

Theorem 1 ([7]). *Let $\mathbf{W} \in \mathbb{C}^{M\times\tau}$ be with i.i.d. entries with $\mathbf{W}_{m,t} \sim \mathcal{CN}(0,\sigma^2)$. Denote by ω_1 the largest eigenvalue of $\frac{1}{\tau}\mathbf{W}\mathbf{W}^{\mathsf{H}}$. Then, as $M \to \infty$, $M/\tau \to c > 0$, for any real x in a compact set*

$$\mathbb{P}\left(\tau^{\frac{2}{3}}\frac{\omega_1 - b}{\tilde{\sigma}} \geq x\right) \to \bar{F}_{TW}(x)$$

where $\bar{F}_{TW}$ is the complementary Tracy–Widom (TW) distribution and

$$b = \sigma^2\left(1+\sqrt{c}\right)^2,\ \tilde{\sigma} = \sigma^2\left(1+\sqrt{c}\right)\left(1+\frac{1}{\sqrt{c}}\right)^{1/3}.$$

In the next sections, $\mathbf{W}$ will correspond to the noise and Theorem 1 will be useful to define a detection test.

Let now $\mathbf{W}$ be perturbed by a low rank matrix $\mathbf{A} \in \mathbb{C}^{M\times\tau}$ (deterministic or random) of fixed rank L as $M \to \infty$ and consider the matrix $\mathbf{Y} = \mathbf{A}+\mathbf{W}$. This model is referred to as a *spiked model* and the spectrum of $\frac{1}{\tau}\mathbf{Y}\mathbf{Y}^{\mathsf{H}}$ still converges to the MP law [8]. However, some eigenvalues can drop out on the right side of the interval $[a,b]$ under some conditions on the singular values of $\mathbf{A}$. The following theorem describes the behavior of the L largest eigenvalues of $\frac{1}{\tau}\mathbf{Y}\mathbf{Y}^{\mathsf{H}}$.

Theorem 2 ([9]). *Let $\mathbf{W} \in \mathbb{C}^{M\times\tau}$ be defined as in Theorem 1. Let $\mathbf{A} \in \mathbb{C}^{M\times\tau}$ be of fixed rank L as $M \to \infty$. Let $a_1 \geq \ldots \geq a_L$ be the singular values of $\mathbf{A}$. Consider the matrix $\mathbf{Y} = \mathbf{A} + \mathbf{W}$ and let $\hat{\lambda}_1 \geq \ldots \geq \hat{\lambda}_M$ be the eigenvalues of $\frac{1}{\tau}\mathbf{Y}\mathbf{Y}^{\mathsf{H}}$. Then, for $l = 1, \ldots, L$, as $M \to \infty$, $M/\tau \to c > 0$,*

$$\hat{\lambda}_l \xrightarrow{a.s.} \begin{cases} \rho_l \triangleq \left(1+\frac{a_l^2}{\sigma^2}\right)\left(1+\frac{c\sigma^2}{a_l^2}\right) & \text{if } a_l^2 > \sigma^2\sqrt{c} \\ b & \text{otherwise.} \end{cases}$$

From Theorem 2, if the singular value a_l of the perturbation matrix is large enough, the corresponding sample covariance eigenvalue $\hat{\lambda}_l$ will converge to the limit ρ_l which is located outside (on the right side) of the MP law's support. Note also that the limit ρ_l depends on a_l^2, σ^2, and on the limiting ratio c. In this paper, the perturbation matrix $\mathbf{A}$ will correspond to the sum of the signal and of the jamming matrices, as these will be of fixed ranks as $M \to \infty$. This is discussed in more details in the next section where a detection of the jamming attack is proposed.

IV. ATTACK DETECTION

In this section we propose an algorithm to detect the presence of a jamming attack.

IV-A. Problem statement

We denote by $\mathcal{H}_0$ the null hypothesis under which there is no attack and by $\mathcal{H}_1$ the alternative hypothesis where there is a jammer. The hypothesis testing problem is given by:

$$\begin{aligned} &\mathcal{H}_0 : \text{absence of jamming} \\ &\mathcal{H}_1 : \text{presence of jamming.} \end{aligned}$$

Considering the transmission scenario of Section II and concatenating the received vectors $\mathbf{y}_t \in \mathbb{C}^{M\times 1}$ at BS for $t = 1, \ldots, \tau$, we obtain the following hypothesis test:

$$\begin{aligned} \mathcal{H}_0 &: \mathbf{Y} = \mathbf{H}\mathbf{X} + \mathbf{W} \\ \mathcal{H}_1 &: \mathbf{Y} = \mathbf{H}\mathbf{X} + \mathbf{H}^{\mathsf{J}}\mathbf{X}^{\mathsf{J}} + \mathbf{W} \end{aligned} \tag{1}$$

where $\mathbf{Y} = [\mathbf{y}_1, \ldots, \mathbf{y}_\tau] \in \mathbb{C}^{M\times\tau}$, $\mathbf{X} = [\mathbf{x}_1, \ldots, \mathbf{x}_\tau] \in \mathbb{C}^{K\times\tau}$, $\mathbf{X}^{\mathsf{J}} = [\mathbf{x}_1^{\mathsf{J}}, \ldots, \mathbf{x}_\tau^{\mathsf{J}}] \in \mathbb{C}^{K^{\mathsf{J}}\times\tau}$, and $\mathbf{W} = [\mathbf{w}_1, \ldots, \mathbf{w}_\tau] \in \mathbb{C}^{M\times\tau}$. In the sequel, it is assumed that M, τ, and K are known to the BS and K^{J} is unknown. Note that both the matrices $\mathbf{H}\mathbf{X}$ and $\mathbf{H}^{\mathsf{J}}\mathbf{X}^{\mathsf{J}}$ are of fixed ranks equal to, respectively, K and K^{J} a.s., as $M \to \infty$. Hence, the model (1) can be viewed, under both $\mathcal{H}_0$ and $\mathcal{H}_1$, as a spiked model. Define the sample covariance matrix by $\widehat{\mathbf{R}} \triangleq \frac{1}{\tau}\mathbf{Y}\mathbf{Y}^{\mathsf{H}}$. The detection is based on the analysis of the largest eigenvalues of $\widehat{\mathbf{R}}$ described in Section III with $\mathbf{A} = \mathbf{H}\mathbf{X}$ with singular values converging to $\sqrt{\tau M P_1}, \ldots, \sqrt{\tau M P_K}$ as $M \to \infty$ (under $\mathcal{H}_0$) and

[1]We assume that the pathlosses $\beta_1, \ldots, \beta_K$ between the users and the BS and $\gamma_1, \ldots, \gamma_{K^{\mathsf{J}}}$ between the jamming devices and the BS are absorbed into $\mathbf{P}$ and $\mathbf{P}^{\mathsf{J}}$, respectively.

$\mathbf{A} = \mathbf{H}\mathbf{X} + \mathbf{H}^{\mathsf{J}}\mathbf{X}^{\mathsf{J}}$ with singular values converging to $\sqrt{\tau M P_1}, \ldots, \sqrt{\tau M P_K}, \sqrt{\tau M P_1^{\mathsf{J}}}, \ldots, \sqrt{\tau M P_{K^{\mathsf{J}}}^{\mathsf{J}}}$ as $M \to \infty$ (under $\mathcal{H}_1$). From Section III, in absence of the signal and the jammer, the spectrum of $\widehat{\mathbf{R}}$ is composed from a noise bulk of eigenvalues converging to the MP law. Recall that a.s., as $M \to \infty$, no eigenvalue due to the noise can be found outside $[a, b]$. Hence, if isolated eigenvalues appear they correspond to the signal (under $\mathcal{H}_0$) and to the signal-plus-jamming (under $\mathcal{H}_1$). Under $\mathcal{H}_0$, up to K isolated eigenvalues due to the users' signals can be found away from the noise bulk. Under $\mathcal{H}_1$, up to $K + K^{\mathsf{J}}$ isolated eigenvalues can appear and they are due to both the signal and the jamming parts. In the following, it will be assumed $P_K > \sigma^2\sqrt{c}/M$ and $P_{K^{\mathsf{J}}}^{\mathsf{J}} > \sigma^2\sqrt{c}/M$, meaning that the received powers from all the users' and jammer's antennas are large enough so they generate $K + K^{\mathsf{J}}$ isolated eigenvalues (see Theorem 2). Otherwise, the user and the jamming signals are negligible compared to the noise and can be ignored. This is observed in Fig. 2 where under $\mathcal{H}_0$ we have $K = 2$ signal eigenvalues and under $\mathcal{H}_1$ there are $K + K^J = 4$ signal-plus-jamming eigenvalues.

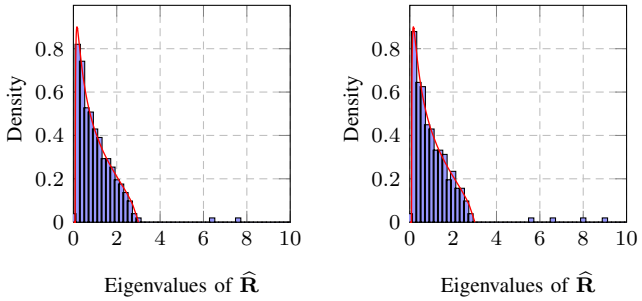

Fig. 2. Histogram of the eigenvalues of $\widehat{\mathbf{R}}$ and the MP law (plane curve) under $\mathcal{H}_0$ (left) and under $\mathcal{H}_1$ (right) for $K = 2$, $K^{\mathsf{J}} = 2$, $M = 256$, and $\tau = 512$, $c = 0.5$, $P_1 = P_2 = 0.02$, $P_1^{\mathsf{J}} = P_1^{\mathsf{J}} = 0.025$, and $\sigma^2 = 1$.

IV-B. Estimation of the jamming subspace

We propose first to estimate the jamming subspace dimension. From Theorem 1, in the absence of the signal and the jammer, the distribution of the largest eigenvalue of the noise covariance matrix converges to a centered and scaled TW distribution as $M \to \infty$. This motivates us to perform a multiple hypothesis testing similarly to the approach of [10] which was proposed in a different context of source enumeration. Let $\hat{\lambda}_1 \geq \ldots \geq \hat{\lambda}_M$ be the eigenvalues of $\widehat{\mathbf{R}}$ and assume σ^2 known at the BS. Since it is assumed that $P_K > \sigma^2\sqrt{c}/M$, there will be at least K isolated eigenvalues corresponding to the signals. Hence, it is sufficient to start the test from the $(K+1)$th largest eigenvalue. We consider the following hypothesis testing, for $k = K+1, \ldots, M$:

$\mathcal{H}_0$: at most $k - 1 - K$ jamming signals present
$\mathcal{H}_1$: at least $k - K$ jamming signals present

where at each sequence of hypothesis test, the kth largest eigenvalue of $\widehat{\mathbf{R}}$ is tested. The hypothesis H_0 is rejected if $\hat{\lambda}_k$ is too large:

$$\hat{\lambda}_k \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\lessgtr}} \xi(\alpha)$$

where ξ is the detection threshold, which is a function of the false alarm rate denoted by α, defined by $\xi(\alpha) \triangleq b + \tau^{-2/3}\bar{F}_{TW}^{-1}(\alpha)\tilde{\sigma}$ with $\tilde{\sigma}$ given in Theorem 1. The testing is stopped at the smallest index k such that $\hat{\lambda}_k < \xi(\alpha)$. Note that it was shown in [10], under hypothesis $\mathcal{H}_0$ of $k - 1 - K$ jamming signals, $\hat{\lambda}_k$ approximately follows the centered and scaled Tracy–Widom as the influence of the first $k - 1$ jamming and/or users' signals can be neglected.

Based on the above discussions, we can now define the estimate of the jamming space dimension K^{J} given by

$$\hat{K^{\mathsf{J}}} = \underset{K+1 \leq k \leq M}{\arg\max} \{\hat{\lambda}_k > \xi(\alpha)\} - K.$$

It can be shown (see for instance [10]) that as $M \to \infty$, $\widehat{K}_{\mathsf{J}}$ is a consistent estimate of K^{J} if $P_{K^{\mathsf{J}}}^{\mathsf{J}} > \sigma^2\sqrt{c}/M$.

IV-C. Jamming detection

We rewrite now the hypothesis testing problem of (1) as:

$$\begin{aligned} \mathcal{H}_0 &: \ \hat{K^{\mathsf{J}}} = 0 \\ \mathcal{H}_1 &: \ \hat{K^{\mathsf{J}}} \geq 1. \end{aligned} \tag{2}$$

It is now straightforward to conclude that an attack is declared if $\hat{K^{\mathsf{J}}} \geq 1$ and absence of an attack in the case where $\hat{K^{\mathsf{J}}} = 0$. The performance of this detector is analyzed in the simulation part and is compared to a classical information theoretic criteria-based approach.

V. JAMMIMG REJECTION

In this section we consider the model (1) under hypothesis $\mathcal{H}_1$ where the jamming attack is present and develop an algorithm to reject interference.

V-A. Subspace estimation

Let $\hat{\lambda}_1 \geq \hat{\lambda}_2 \geq \ldots \geq \hat{\lambda}_{K+K^{\mathsf{J}}}$ be the largest eigenvalues of $\widehat{\mathbf{R}}$. Assume for all $k \in \{1, \ldots, K\}$ and all $k^{\mathsf{J}} \in \{1, \ldots, K^{\mathsf{J}}\}$, P_k and $P_{k^{\mathsf{J}}}^{\mathsf{J}}$ are distinct with P_k known at the BS and P_k^{J} unknown. Let $q_1, \ldots, q_K$ be the indices of the eigenvalues corresponding to the K users. From Theorem 2, for $k = 1, \ldots, K$, as $M \to \infty$, we have

$$\hat{\lambda}_{q_k} \xrightarrow{\text{a.s.}} \rho_k = \left(1 + \frac{MP_k}{\sigma^2}\right)\left(1 + \frac{c\sigma^2}{MP_k}\right).$$

We propose now to identify the K eigenvalues among the $K + K^{\mathsf{J}}$ eigenvalues corresponding to the users. Define the normalized mean square error (NMSE) of the kth eigenvalue, for $k = 1, \ldots, K + K^{\mathsf{J}}$, as

$$\text{NMSE}(k) \triangleq \frac{\left|\hat{\lambda}_k - \rho_k\right|^2}{\rho_k^2}.$$

We denote by i_k the index of the eigenvalue having the i_kth smallest NMSE. As all the users' and jammer's powers are assumed to be distinct, the indices corresponding to the K smallest NMSE (and hence corresponding to the K users' eigenvalues) are given by

$$\begin{aligned} i_1 &= \underset{l\in\{1,\ldots,K+K^{\mathsf{J}}\}}{\arg\min} \ \text{NMSE}(l) \\ &\vdots \\ i_k &= \underset{l\in\{1,\ldots,K+K^{\mathsf{J}}\}\setminus\{i_1,\ldots,i_{k-1}\}}{\arg\min} \ \text{NMSE}(l) \\ &\vdots \\ i_K &= \underset{l\in\{1,\ldots,K+K^{\mathsf{J}}\}\setminus\{i_1,\ldots,i_{K-1}\}}{\arg\min} \ \text{NMSE}(l). \end{aligned}$$

Denote by $\hat{\mathbf{u}}_{i_1},\ldots,\hat{\mathbf{u}}_{i_K}$ the eigenvectors of $\widehat{\mathbf{R}}$ corresponding to the eigenvalues $\hat{\lambda}_{i_1} \geq \ldots \geq \hat{\lambda}_{i_K}$. We define the orthogonal projector $\mathbf{\Pi} \in \mathbb{C}^{M\times K}$ on the signal subspace generated by $\hat{\mathbf{u}}_{i_1},\ldots,\hat{\mathbf{u}}_{i_K}$ as

$$\mathbf{\Pi} \triangleq [\hat{\mathbf{u}}_{i_1},\ldots,\hat{\mathbf{u}}_{i_K}].$$

V-B. Subspace projected channel estimation

We consider the transmission over the coherence interval τ where τ_p is the duration of the pilot sequence such that $\tau_p \geq K$ and $\tau_d = \tau - \tau_p$ is the duration of the data sequence. We recall that in this case the transmission model is given by

$$\mathbf{Y} = \mathbf{H}\mathbf{X} + \mathbf{H}^{\mathsf{J}}\mathbf{X}^{\mathsf{J}} + \mathbf{W} \tag{3}$$

where now $\mathbf{X} = [\mathbf{X}_p \ \mathbf{X}_d]$ with $\mathbf{X}_p \in \mathbb{C}^{K\times\tau_p}$ the matrix of orthogonal pilots such that $\mathbf{X}_p\mathbf{X}_p^{\mathsf{H}} = \tau_p\mathbf{I}_K$, $\mathbf{X}_d \in \mathbb{C}^{K\times\tau_d}$ is the transmitted signal matrix with entries defined as in Section IV, $\mathbf{X}^{\mathsf{J}} = [\mathbf{X}_p^{\mathsf{J}} \ \mathbf{X}_d^{\mathsf{J}}]$ is the jamming signal matrix with $\mathbf{X}_p^{\mathsf{J}} \in \mathbb{C}^{K^{\mathsf{J}}\times\tau_p}$ and $\mathbf{X}_d^{\mathsf{J}} \in \mathbb{C}^{K^{\mathsf{J}}\times\tau_d}$ the signals transmitted during the pilot and data phases, respectively; $\mathbf{W} = [\mathbf{W}_p \ \mathbf{W}_d]$ with $\mathbf{W}_p \in \mathbb{C}^{M\times\tau_p}$ and $\mathbf{W}_d \in \mathbb{C}^{M\times\tau_d}$ are the noise matrices for pilot and data phases, respectively; $\mathbf{Y} = [\mathbf{Y}_p \ \mathbf{Y}_d]$ with $\mathbf{Y}_p \in \mathbb{C}^{M\times\tau_p}$ and $\mathbf{Y}_d \in \mathbb{C}^{M\times\tau_d}$ the signals received during the pilot and data phases, respectively; finally, the channel matrices are defined as previously. Similarly to the algorithm of [11], we project the received data signal matrix onto the estimated signal subspace in order to reject the jamming (and noise):

$$\widetilde{\mathbf{Y}} = \mathbf{\Pi}^{\mathsf{H}}\mathbf{Y}_d = \mathbf{\Pi}^{\mathsf{H}}\mathbf{H}\mathbf{X}_d + \mathbf{\Pi}^{\mathsf{H}}\mathbf{H}^{\mathsf{J}}\mathbf{X}_d^{\mathsf{J}} + \mathbf{\Pi}^{\mathsf{H}}\mathbf{W}_d.$$

Notice that the channel estimation problem reduces to estimation of the $K \times K$ matrix

$$\widetilde{\mathbf{H}} = \mathbf{\Pi}^{\mathsf{H}}\mathbf{H}.$$

The estimate can be obtained by least squares using τ_p pilot sequences as:

$$\widehat{\widetilde{\mathbf{H}}} = \frac{1}{\tau_p}\mathbf{\Pi}^{\mathsf{H}}\mathbf{Y}_p\mathbf{X}_p^{\mathsf{H}}\mathbf{P}^{-\frac{1}{2}}.$$

V-C. Performance analysis

We analyze the performance in terms of spectral efficiency under linear detection. A spectral efficiency [12] for user $k = 1,\ldots,K$ is given by

$$\mathcal{S}_k = \left(1 - \frac{\tau_p}{\tau_c}\right)\log_2\left(1 + \frac{\left|\mathbb{E}\left[\mathbf{b}_k^{\mathsf{H}}\tilde{\mathbf{h}}_k\right]\right|^2 P_k}{\frac{\mathbb{E}\left[\|\bar{\mathbf{y}}_k\|^2\right]}{\tau_c-\tau_p} - \left|\mathbb{E}\left[\mathbf{b}_k^{\mathsf{H}}\tilde{\mathbf{h}}_k\right]\right|^2 P_k}\right) \tag{4}$$

where $\mathbf{b}_k \in \mathbb{C}^{K\times 1}$ is the detection vector, $\tilde{\mathbf{h}}_k \in \mathbb{C}^{K\times 1}$ is the kth column of $\widetilde{\mathbf{H}}$, and $\bar{\mathbf{y}}_k = \mathbf{b}_k^{\mathsf{H}}\widetilde{\mathbf{Y}} \in \mathbb{C}^{K\times\tau_d}$ is the filtered received vector for user k. An approximate minimum mean square error (MMSE) detection filter for user $k = 1,\ldots,K$ is given by

$$\mathbf{b}_k^{\text{MMSE}} = \hat{\tilde{\mathbf{h}}}_k\mathbf{P}^{\frac{1}{2}}\left(\mathbf{P}^{\frac{1}{2}}\hat{\tilde{\mathbf{h}}}_k^{\mathsf{H}}\hat{\tilde{\mathbf{h}}}_k\mathbf{P}^{\frac{1}{2}} + \sigma^2\mathbf{I}_K\right)^{-1}$$

where $\hat{\tilde{\mathbf{h}}}_k \in \mathbb{C}^{K\times 1}$ is the kth column of $\widehat{\widetilde{\mathbf{H}}}$.

VI. SIMULATION RESULTS

In this section we provide simulation results for $K = 2$ and $K^{\mathsf{J}} = 2$ with equal received user powers ($P_1 = P_2 = P$) and equal received jamming powers ($P_1^{\mathsf{J}} = P_2^{\mathsf{J}} = P^{\mathsf{J}}$). We analyze first the performance of the proposed jamming detection algorithm. The probability of false alarm is set to $\alpha = 0.01$ and the hypothesis test given by (2) is performed. In Fig. 3, the correct detection rates (CDR) versus P^{J} (dB) for different τ are plotted for $P = -10$ dB. The results are compared to the minimum description length (MDL) [13] method relying on the closeness of the $M-(K+K^{\mathsf{J}})$ noise eigenvalues of $\widehat{\mathbf{R}}$. We observe that the proposed algorithm outperforms the MDL approach by 5 dB meaning that weaker jamming signals can be detected.

In Figs. 4–5, the performance of the jamming rejection algorithm (*Proposed I*) from Section V is shown in terms of spectral efficiency (bits/s/Hz) and compared to the spectral efficiency obtained in the following scenarios: (i) *Jamming* (under attack); (ii) *Jamming free* case (no attack); (iii) *Proposed II* case (the rejection algorithm is applied to the jamming free model). In Fig. 4 the spectral efficiency for one user (1 or 2) is plotted versus SNR $= P/\sigma^2$ (dB) whereas in Fig. 5 they are drawn versus P^{J} (dB). In all plots similar behaviors are observed where the performance of the proposed algorithm is drastically degraded when P and P^{J} are close. This is explained by the fact that when $P = P^{\mathsf{J}}$, the corresponding signal and jamming isolated eigenvalues converge to the same limit and hence, the signal subspace cannot be well estimated and separated from the jamming. Notice however that at low SNR (or low P^{J}) the proposed method shows a particularly better performance than both the jamming case and the case where no attack is present. Indeed, the rejection algorithm rejects not only the jamming but also the noise by projecting the received signal to the signal subspace. In summary, the proposed method displays

a very good performance when $P \gg P^{\mathsf{J}}$ or $P^{\mathsf{J}} \gg P$. The latter shows that a dumb jammer that uses very high power can easily be rejected.

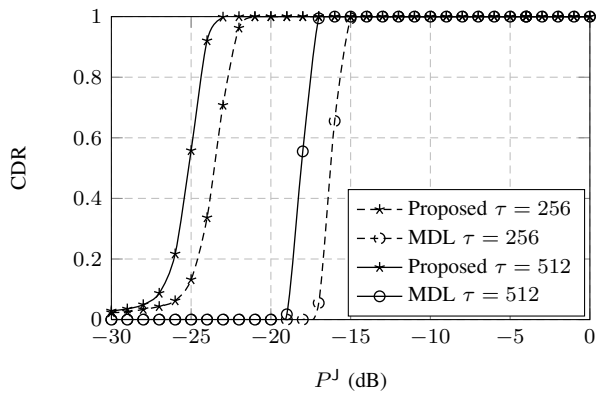

Fig. 3. CDR for user 1 versus SNR (dB) with $K = 2$, $K^{\mathsf{J}} = 2$, $M = 256$, $P = -10$ dB, and $\sigma^2 = 0$ dB.

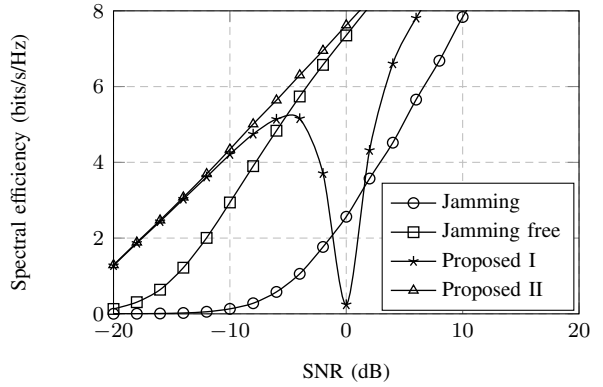

Fig. 4. Spectral efficiency of user 1 (or 2) versus SNR (dB) with $K = 2$, $K^{\mathsf{J}} = 2$, $M = 256$, $\tau = 512$, $c = 0.5$, $P^{\mathsf{J}} = 0$ dB, and $\sigma^2 = 0$ dB.

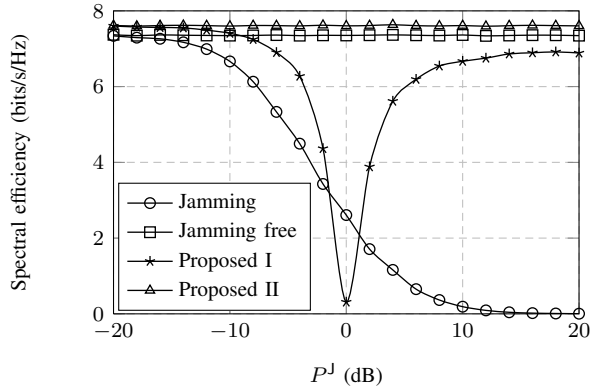

Fig. 5. Spectral efficiency of user 1 (or 2) versus P^{J} (dB) with $K = 2$, $K^{\mathsf{J}} = 2$, $M = 256$, $\tau = 512$, $c = 0.5$, $P = 0$ dB, and $\sigma^2 = 0$ dB.

VII. CONCLUSION

The results confirm the vulnerability of massive MIMO to attacks in the pilot transmission phase. Nevertheless, the BS can detect the jamming and reject it when the power levels of the desired signals and jamming are sufficiently different. We observed that if the jammer smartly adjusts its transmission power to match the desired signals, the spectral efficiency is drastically affected. This motivates to analyze the effect of other configurations of jamming devices, in particular, massive jamming with a large number of (un)coordinated antennas K^{J}, of the same order of magnitude as M.

VIII. REFERENCES

[1] E. G. Larsson, O. Edfors, F. Tufvesson, and T. L. Marzetta, "Massive MIMO for next generation wireless systems," *IEEE Comm. Mag.*, vol. 52, no. 2, pp. 186–195, 2014.

[2] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Comm. Mag.*, vol. 53, pp. 21–27, 2015.

[3] Y. O. Basciftci, C. E. Koksal, and A. Ashikhmin, "Securing massive MIMO at the physical layer," in *IEEE CNS*, pp. 272–280, 2015.

[4] H. Pirzadeh, S. M. Razavizadeh, and E. Björnson, "Subverting massive MIMO by smart jamming," *Wireless Comm. Letters*, vol. 5, no. 1, pp. 20–23, 2016.

[5] V. A. Marčenko and L. A. Pastur, "Distribution of eigenvalues for some sets of random matrices," *Mathematics of the USSR-Sbornik*, vol. 1, no. 4, pp. 457–483, 1967.

[6] Z. D. Bai and J. W. Silverstein, "No eigenvalues outside the support of the limiting spectral distribution of large-dimensional sample covariance matrices," *Ann. Probab.*, vol. 26, no. 1, pp. 316–345, 1998.

[7] K. Johansson, "Shape fluctuations and random matrices," *Comm. in Math. Physics*, vol. 209, pp. 437–476, 2000.

[8] Z. D. Bai, "Methodologies in spectral analysis of large-dimensional random matrices, a review," *Statististica Sinica*, vol. 9, pp. 611–677, 1999.

[9] J. Baik and J. W. Silverstein, "Eigenvalues of large sample covariance matrices of spiked population models," *J. Multivariate Anal.*, vol. 97, no. 6, pp. 1382–1408, 2006.

[10] S. Kritchman and B. Nadler, "Non-parametric detection of the number of signals: hypothesis testing and random matrix theory," *IEEE Trans. on Sig. Proc.*, vol. 57, no. 10, pp. 3930–3941, 2009.

[11] H. Q. Ngo and E. G. Larsson, "EVD-based channel estimation in multicell multiuser MIMO systems with very large antenna arrays," in *IEEE ICASSP*, pp. 3249–3252, 2012.

[12] J. Jose, A. E. Ashikhmin, T. L. Marzetta, and S. Vishwanath, "Pilot contamination and precoding in multi-cell TDD systems," *IEEE Trans. on Wireless Comm.*, vol. 10, no. 8, pp. 2640–2651, 2011.

[13] M. Wax and T. Kailath, "Detection of signals by information theoretic criteria," *IEEE Trans. on ASSP*, vol. 33, no. 2, pp. 387–392, 1985.